

REMARKS

In the Office Action, the Examiner rejected claim 28 under 35 U.S.C. § 103(a) as unpatentable over Bowman (U.S. Patent No. 5,627,886); and rejected claims 1-3, 5-27, 29-33, and 35-66 under 35 U.S.C. § 103(a) as unpatentable over Bowman in view of Phelps (U.S. Patent No. 5,602,906). Applicants respectfully traverse the Examiner's rejections under 35 U.S.C. § 103(a). Claims 1-3, 5-33, and 35-66 remain pending.

REJECTION UNDER 35 U.S.C. § 103(a) BASED ON BOWMAN

On page 8 of the Office Action, the Examiner rejected claim 28 under 35 U.S.C. § 103(a) as allegedly unpatentable over Bowman. Applicants respectfully traverse this rejection.

Independent claim 28 is directed to a system for monitoring one or more of a plurality of credit card or debit card networks, each network being configured to generate network event records, each network event record being generated in response to an event occurring in the network. The system comprises a fraud detection system including a core computing infrastructure and a domain specific infrastructure. The domain specific infrastructure is dynamically reconfigurable in accordance with the domain specific implementation of the network being monitored. The core computing infrastructure is non-domain specific. The fraud detection system is configured to determine whether the network is a credit card network or a debit card network, to analyze each network event record, and to perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on the determination of whether the network is a credit card network or a debit card network.

Bowman does not disclose or suggest the combination of features recited in claim 28. For example, Bowman does not disclose or suggest a fraud detection system configured to determine whether the network is a credit card network or a debit card network, to analyze each

network event record, and to perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on the determination of whether the network is a credit card network or a debit card network, as required by claim 28. Instead, Bowman discloses a fraud detection system for detecting and preventing fraudulent use of communications or credit card/business networks (col. 2, lines 45-47). Indeed, the words “debit card” do not appear in Bowman.

The Examiner failed to address the underlined language recited above in claim 28. For example, the Examiner alleged:

As per **claim 28**, Bowman discloses a system for monitoring one or more of a plurality of credit card or debit card networks, each network being configured to generate network event records, each network event record being generated in response to an event occurring in the network, the system comprising:

a fraud detection system including a core computing infrastructure (configurable software for configuring the disparate networks) and a domain specific infrastructure (configurable software or object oriented software for defining user specific data/rules), the domain specific infrastructure being dynamically reconfigurable in accordance with the domain specific implementation of the network being monitored, the core computing infrastructure being non-domain specific (configurable software for disparate networks), the fraud detection system being configured to analyze each network event record and perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on whether the network is a credit card network or debit card network....

(Office Action, pages 8 and 9). Nowhere in the allegation does the Examiner address a fraud detection system configured to determine whether the network is a credit card network or a debit card network, to analyze each network event record, and to perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on the determination of whether the network is a credit card network or a debit card network, as required by claim 28. Applicants respectfully submit that the Examiner is unable to address these features of claim 28 because Bowman fails to disclose or remotely suggest them.

As shown by the reproduced portion the Office Action, the Examiner appeared to allege that Bowman teaches the fraud detection system recited in claim 28, and cited Fig. 2, col. 2, lines 40-67, and col. 3, lines 5-40 of Bowman for support (Office Action, pages 8 and 9). Applicants respectfully disagree with the Examiner's interpretation of Bowman.

Col. 5, line 19 - col. 6, line 32 of Bowman discusses Fig. 2 and discloses the architecture of the fraud management system (FMS), and that the FMS (and thus Fig. 2) is limited to detecting and preventing fraudulent use of communications or credit card/business networks. Nowhere in this section, or elsewhere, does Bowman disclose or suggest a fraud detection system configured to determine whether the network is a credit card network or a debit card network, to analyze each network event record, and to perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on the determination of whether the network is a credit card network or a debit card network, as required by claim 28.

Col. 2, lines 40-67 of Bowman states:

The Fraud Management System (FMS) of the present invention effectively detects usage patterns indicative of many types of known fraud including: calling card related fraud, cellular phone fraud, subscription fraud, hacking, call selling, 900/800 fraud, and PBX or CPE fraud, among others. As a result, the FMS provides a means for detecting and ultimately preventing fraudulent use of communications or credit card/business networks. Monitoring network usage for fraudulent telecommunications network usage patterns according to the present invention takes place outside the switch and normally after the call event has completed.

The system monitors network usage on an event-by-event basis, accepting event record detail information from multiple network sources. As fraud is dynamic, exploiting new technologies and services nearly as quickly as they are deployed, the system also possesses a high degree of configurability. Fraud system administrators are able to create new detection mechanisms without the need to write new programs. Finally, the system and method of the present invention supports an analysis of trends in network usage, so that "early warnings" of new types of fraud are available.

The system and method of the present invention assists in detecting fraudulent use of a communications network by monitoring the network to detect usage patterns typically

indicative of fraud. The present system is not limited to detecting the types of fraud known to exist today. It is a general-purpose system that can be configured to detect many different sorts of usage patterns.

In this section, Bowman discloses a fraud management system (FMS) for detecting and preventing fraudulent use of communications or credit card/business networks. Nowhere in this section, or elsewhere, does Bowman disclose or suggest a fraud detection system configured to determine whether the network is a credit card network or a debit card network, to analyze each network event record, and to perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on the determination of whether the network is a credit card network or a debit card network, as required by claim 28.

Col. 3, lines 5-40 of Bowman states:

For example, as new customers are added to the network, the system accommodates them without disruption of service. The system is flexible enough to change as existing customers' network service requirements change, and can be tailored to their specific needs. As new networks services become available, the system can be readily updated to detect new types of fraud associated with those services. Moreover, as new sources of data become available for analysis, they can be easily integrated into the FMS without re-engineering existing system components.

The system architecture of the present invention is preferably built upon an object-oriented foundation. Each major system component is composed of a set of objects, which encapsulate both data and behavior. For the system administrator, this strategy provides reusable data structures which may be used as templates to simplify the configuration process. For the engineers who must maintain the system, this strategy minimizes the impact of coding changes, promotes the sharing of common code, and makes maintenance tasks much easier.

The fraud monitoring system and method of the present invention is quite useful to, for example, telecommunications carriers that are handling both wireless and wireline communications (including digital cellular and analog cellular network combinations). This is because all of the traffic of all of their subscribers is consolidated in one information repository. By way of illustration, when a carrier finds someone committing fraud, it will want to consider reviewing numbers they are calling. Moreover one wonders who is calling them. Before the present invention, one would have to check more than one repository for this information. The system and method of the present invention has all of the information regardless of network or type of transaction in one repository; such information can be quickly and easily obtained.

In this section, Bowman discloses a fraud management system (FMS) for detecting and

preventing fraudulent use of communications or credit card/business networks. Nowhere in this section, or elsewhere, does Bowman disclose or suggest a fraud detection system configured to determine whether the network is a credit card network or a debit card network, to analyze each network event record, and to perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on the determination of whether the network is a credit card network or a debit card network, as required by claim 28.

For at least these reasons, Applicants submit that claim 28 is patentable over Bowman. Applicants, therefore, respectfully request the reconsideration and withdrawal of the 35 U.S.C. § 103(a) rejection of claim 28 as allegedly unpatentable over Bowman.

REJECTION UNDER 35 U.S.C. § 103(a) BASED ON BOWMAN AND PHELPS

On page 9 of the Office Action, the Examiner rejected claims 1-3, 5-27, 29-33, and 35-66 under 35 U.S.C. § 103(a) as allegedly unpatentable over Bowman in view of Phelps. Applicants respectfully traverse this rejection.

Independent claim 1, for example, is directed to a method for detecting fraud in one of a credit card or debit card system. The system generates network event records, where each network event record is generated in response to an event in the system. The method includes determining whether the system is a credit card system or a debit card system, performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, and generating a fraud alarm upon detection of suspected fraud by the at least one fraud detection test. The method also includes correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud, and responding to the fraud case with a fraud prevention action,

the fraud prevention action being based on the priority assigned to the fraud case.

Bowman and Phelps, whether taken alone or in any reasonable combination, do not disclose or suggest the combination of features recited in claim 1. For example, Bowman does not disclose or suggest a method for detecting fraud in one of a credit card or debit card system that includes determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as required by claim 1. Instead, Bowman discloses a fraud detection system for detecting and preventing fraudulent use of communications or credit card/business networks (col. 2, lines 45-47). Indeed, the words “debit card” do not appear in Bowman. Thus, Bowman cannot disclose or suggest, *inter alia*, determining whether a system is a credit card system or a debit card system, as recited in claim 1.

The Examiner failed to address the underlined language recited above in claim 1. For example, the Examiner alleged:

As per claim 1, Bowman discloses a method for detecting fraud in one of a credit card or debit card system, the system generating network event records, each network event record being generated in response to an event in the system, the method comprising the steps of:

(1) performing at least one fraud detection test on the network event records based on whether the system is a credit card system or a debit card system (see fig. 2; col. 2, lines 15-25,40-50; col. 3, line 60-col. 4, line 5; col. 17, lines 1-10 ... detecting network usage pattern indicative of fraud ... credit card usage and authorization records...);

(Office Action, page 10). Nowhere in the allegation does the Examiner address determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as required by claim 1. Applicants

respectfully submit that the Examiner is unable to address these features of claim 1 because Bowman fails to disclose or remotely suggest them.

As shown by the reproduced portions the Office Action, the Examiner appeared to allege that Bowman discloses performing at least one fraud detection test on the network event records based on whether the system is a credit card system or a debit card system, and cited Fig. 2, col. 2, lines 15-25 and 40-50, col. 3, line 60 - col. 4, line 5, and col. 17, lines 1-10 of Bowman for support (Office Action, page 10). Applicants respectfully disagree with the Examiner's interpretation of Bowman.

Col. 5, line 19 - col. 6, line 32 of Bowman discusses Fig. 2 and discloses the architecture of the FMS. For example, at col. 5, line 60 - col. 6, line 5, Bowman states:

An event record is a collection of data fields which describes an instance of network usage. Each event record contains all of the information about a call event that the system uses. FMS 10 preferably assigns each call event record an event type or category, based on the types of network services the record reflects. FMS 10 considers call events to be atomic (i.e., call events cannot span records). The following are some examples of event types: IDD calls, calling card calls, automatic collect calls, information services, other services, digital cellular calls, digital cellular forwarded calls, analog cellular calls, roaming calls. Other examples include event types resulting from the use of a video network, use of a data network or other use of a voice network.

In this section, Bowman discloses that a fraud management system (FMS) (and thus Fig. 2) is limited to detecting and preventing fraudulent use of communications or credit card/business networks. Nowhere in this section, or elsewhere, does Bowman disclose or suggest a method for detecting fraud in one of a credit card or debit card system that include determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as required by claim 1.

Col. 2, lines 15-25 of Bowman states:

It is a further object of the present invention to provide a system and method for detecting network usage patterns indicative of fraud wherein such system and method support any combination of a plurality of disparate networks. Each of the networks are sources of respective network event records reflecting use of such network. Examples of such event records include call detail records from wireline, digital or analog cellular communications networks, or credit card usage and authorization records, roaming data (typically either real-time or via tape), video data, communications data, etc.

In this section, Bowman discloses a system and method for detecting fraud in wireline, digital or analog cellular communications networks, or credit card usage and authorization records, roaming data, video data, communications data, etc. Nowhere in this section, or elsewhere, does Bowman disclose or suggest a method for detecting fraud in one of a credit card or debit card system that includes determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as required by claim 1.

At col. 2, lines 40-50, Bowman states:

The Fraud Management System (FMS) of the present invention effectively detects usage patterns indicative of many types of known fraud including: calling card related fraud, cellular phone fraud, subscription fraud, hacking, call selling, 900/800 fraud, and PBX or CPE fraud, among others. As a result, the FMS provides a means for detecting and ultimately preventing fraudulent use of communications or credit card/business networks. Monitoring network usage for fraudulent telecommunications network usage patterns according to the present invention takes place outside the switch and normally after the call event has completed.

In this section, Bowman discloses a fraud management system (FMS) for detecting and preventing fraudulent use of communications or credit card/business networks. Nowhere in this section, or elsewhere, does Bowman disclose or suggest a method for detecting fraud in one of a credit card or debit card system that includes determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit

card system, as required by claim 1. Indeed, Bowman cannot disclose this feature of claim 1 because the reference fails to disclose the words “debit card.”

Col. 3, line 60 - col. 4, line 5 of Bowman states:

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The system and method of the present invention effectively detects network usage patterns often indicative of many types of known fraud, including: calling card-related fraud, cellular phone fraud, subscription fraud, hacking, call selling, 900/800 fraud, PBX or CPE fraud, credit card fraud, etc. While not all unusual patterns of network usage indicate fraud, certain patterns are more likely than not to indicate the possibility of fraud and bear further investigation by a user or fraud analyst. It should be understood at this point that any user referred to herein may also be a system administrator or a fraud analyst, or both.

In this section, Bowman discloses a system and method for detecting fraud, including calling card-related fraud, cellular phone fraud, subscription fraud, hacking, call selling, 900/800 fraud, PBX or CPE fraud, credit card fraud, etc. Nowhere in this section, or elsewhere, does Bowman disclose or suggest a method for detecting fraud in one of a credit card or debit card system that includes determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as required by claim 1.

Col. 17, lines 1-10 of Bowman states:

Frequently the specification of a call event type does not narrow the scope of analysis enough for meaningful conclusions. Additional data criteria, or screenings, are required to produce meaningful statistics. A screening is a test applied to one field in a call event. If the test is true, the screening is passed. For a measurement to produce a non-zero result all screenings attached to the measurement must be passed. FMS 10 supports a variety of types of screenings, including:

List--The screening check performs a comparison against a list of discrete values using the contents of a field in the event.

In this section, Bowman discloses screening a call event. Nowhere in this section, or elsewhere,

does Bowman disclose or suggest a method for detecting fraud in one of a credit card or debit card system, determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as required by claim 1.

While not acquiescing in the Examiner's rejection, Applicants respectfully submit that the disclosure of Phelps does not cure the deficiencies in the disclosure of Bowman identified above with regard to claim 1. For example, Phelps does not disclose or suggest a method for detecting fraud in one of a credit card or debit card system that includes determining whether the system is a credit card system or a debit card system, or performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as required by claim 1. In the Office Action, the Examiner did not rely upon Phelps as disclosing these features of claim 1. Furthermore, Phelps discloses a fraud detection system for use in a telecommunications system to detect unauthorized use of billing numbers (col. 1, lines 6-10). The words "debit card" do not appear in Phelps, and the words "credit card" only appear in Phelps in connection with a billing number of the telecommunications system (col. 2, line 49).

The Examiner further alleged:

... Furthermore it is not necessary that the word "debit card" appear in Bowman because the claim limitation is on the alternative. However, even if the limitation is not in the alternative, it would still be obvious to one of ordinary skill in the art because credit card and debit card use the same network for authorization purposes.

* * *

... Bowman, in addition to the discussion above does disclose a screening means by which call event records are screened. A screening is a test applied to one field in a call event. Bowman's Fraud Management System support a variety of types of screening including list , range , pattern etc....

(Office Action, page 4). Applicants respectfully traverse the Examiner's allegations.

First, whether a system is a credit card system or a debit card system is in the alternative. However, that is why claim 1 recites determining whether the system is a credit card system or a debit card system, and performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system. The determination of whether the system is credit card system or a debit card system is not in the alternative, and nowhere does Bowman disclose or remotely suggest such determination. Indeed, Bowman cannot possibly disclose or suggest determining whether the system is a credit card system or a debit card system, because the reference fails to disclose the words "debit card."

Second, with regard to the Examiner's allegation that "it would still be obvious to one of ordinary skill in the art because credit card and debit card use the same network for authorization purposes", Applicants respectfully submit that the Examiner's allegation is merely a conclusory statement that completely lacks support in Bowman. Such motivation statements are insufficient for establishing a *prima facie* case of obviousness. In this respect, Applicants rely upon KSR International Co. v. Teleflex Inc., 550 U.S. ____ (April 30, 2007) (citing In re Kahn, 441 F.3d 977, 988 (Fed. Cir. 2006)), where it was held that rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.

Finally, while not acquiescing in the Examiner's allegations regarding the screening means of Bowman, Applicants respectfully submit that the screening means of Bowman cannot possibly disclose or suggest performing at least one fraud detection test on the network event records based on the determination of whether the system is a credit card system or a debit card system, as recited in claim 1, because the reference fails to disclose the words "debit card" and

thus fails to disclose or suggest determining whether the system is a credit card system or a debit card system, as further recited in claim 1.

For at least these reasons, Applicants submit that claim 1 is patentable over Bowman and Phelps, whether taken alone or in any reasonable combination. Claims 2, 3, and 5-27 depend from claim 1 and are, therefore, patentable over Bowman and Phelps, whether taken alone or in any reasonable combination, for at least the reasons given with regard to claim 1.

Claims 29-33 and 35-66 depend from claim 28. While not acquiescing in the Examiner's rejection, Applicants respectfully submit that the disclosure of Phelps does not cure the deficiencies in the disclosure of Bowman identified above with regard to claim 28. For example, Phelps does not disclose or suggest a fraud detection system configured to determine whether the network is a credit card network or a debit card network, to analyze each network event record, and to perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on the determination of whether the network is a credit card network or a debit card network, as required by claim 28. In the Office Action, the Examiner did not rely upon Phelps as disclosing these features of claim 28. Furthermore, Phelps discloses a fraud detection system for use in a telecommunications system to detect unauthorized use of billing numbers (col. 1, lines 6-10). The words "debit card" do not appear in Phelps, and the words "credit card" only appear in Phelps in connection with a billing number of the telecommunications system (col. 2, line 49).

For at least these reasons, Applicants submit that claims 29-33 and 35-66 are patentable over Bowman and Phelps, whether taken alone or in any reasonable combination, for at least the reasons given with regard to claim 28.

In light of the above, Applicants respectfully request the reconsideration and withdrawal

of the 35 U.S.C. § 103(a) rejection of claims 1-3, 5-27, 29-33, and 35-66 as allegedly unpatentable over Bowman and Phelps.

CONCLUSION

In view of the foregoing remarks, Applicants respectfully request the Examiner's reconsideration of the application and the timely allowance of pending claims 1-3, 5-33, and 35-66.

As Applicants' remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicants' silence as to assertions by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., whether a reference constitutes prior art, motivation to combine references, assertions as to dependent claims, etc.) is not a concession by Applicants that such assertions are accurate or such requirements have been met, and Applicants reserve the right to analyze and dispute such assertions/requirements in the future.

If the Examiner does not believe that all pending claims are now in condition for allowance, the Examiner is urged to contact the undersigned to expedite prosecution of this application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY SNYDER, L.L.P.

Date: October 8, 2007

By: /James M. Olsen, Reg. No. 40,408/
James M. Olsen
Reg. No. 40,408

11350 Random Hills Road
Suite 600
Fairfax, Virginia 22030
Phone: (302) 478-4548
Fax: (571) 432-0808
CUSTOMER NUMBER: 25537